AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method for providing recipient-end security for transmitted data, the method comprising:

~~scanning a hard copy document with a~~ identifying data ~~transmitting device~~ to ~~generate scanned data~~ be transmitted to a data receiving device of a recipient;

configuring the ~~scanned~~ identified data on ~~the~~ a data transmitting device so as to ~~require recipient-end security such that machine-specific security data that identifies~~ add an executable to the data that, when executed on ~~a~~ the data receiving device, ~~to which the scanned data will be transmitted is verified prior to enabling access to~~ verifies that one or both of the recipient and the data receiving device are authorized to access the transmitted data;

transmitting the ~~scanned~~ identified data and the executable from the data transmitting device to the data receiving device;

~~determining~~ the executable executing on the data receiving device and determining if the transmitted data may be accessed by ~~verifying the machine-specific security data~~ the recipient; and

the executable denying access to the transmitted data if it is determined that the transmitted data may not be accessed.

2. (Canceled)

3. (Currently amended) The method of claim 1, wherein ~~configuring the scanned data further~~ determining if the transmitted data may be accessed comprises ~~configuring the scanned data such that~~ the executable verifying recipient-specific security information ~~must be~~ provided

by ~~a~~ the recipient ~~of the transmitted data prior to accessing the transmitted data~~.

4. (Currently amended) The method of claim 3, wherein ~~configuring the scanned data comprises configuring the scanned data such that the recipient must provide~~ verifying recipient-specific security information comprises verifying recipient biometric information ~~to access the transmitted data~~.

5. (Canceled)

6. (Currently amended) The method of claim 1, wherein ~~configuring the scanned data~~ determining if the transmitted data may be accessed comprises ~~configuring the scanned data such that at least one of~~ the executable verifying one or both of an Internet protocol (IP) address and a media access control (MAC) address of the data receiving device ~~is verified~~.

7-12. (Canceled)

13. (Previously presented) The method of claim 1, further comprising, if it is determined that the transmitted data may be accessed, printing out the transmitted data or opening an email attachment that comprises the transmitted data.

14-19. (Canceled)

20. (Currently amended) A ~~system stored on a computer readable medium~~ data transmitting device~~, the system~~ comprising:

an executable program configured to be transmitted along with identified data to a data receiving device and to execute on the data receiving device when a recipient attempts to access the identified data, the executable program further being configured to verify that one or both of

the recipient and the data receiving device are authorized to access the identified data; and

sender-end logic ~~adapted to execute on a data transmitting device, the sender-end logic being~~ configured to ~~configure data scanned by the data transmitting device so as to require verification of machine-specific security data that identifies a data receiving device to which the scanned data will be transmitted~~ add the executable program to the identified data and transmit the executable program and the identified data to the data receiving device; ~~and~~

~~recipient-end logic adapted to execute on a data receiving device, the recipient-end logic being configured to verify the machine-specific security information of the data receiving device~~.

21. (Currently amended) The ~~system~~ data transmitting device of claim 20, wherein the ~~sender-end logic is further configured to require~~ executable program is configured to verify recipient biometric information ~~of the recipient prior to access of the scanned data~~.

22. (Currently amended) The ~~system~~ data transmitting device of claim 20, wherein the ~~sender-end logic~~ executable program is configured to verify ~~at least~~ one or both of an Internet protocol (IP) address and a media access control (MAC) address of the data receiving device.

23-31. (Canceled)

32. (New) A data receiving device, comprising:

recipient-end logic configured to

receive identified data and an executable program from a data transmitting device, and

execute the executable program on the data receiving device when a recipient attempts to access the identified data at the data receiving device, the executable program configured to verify that one or both of the recipient and the data receiving device are authorized to access the identified data.

33. (New) The data receiving device of claim 32, wherein the executable program is configured to verify recipient biometric information.

34. (New) The data receiving device of claim 32, wherein the executable program is configured to verify one or both of an Internet protocol (IP) address and a media access control (MAC) address of the data receiving device.

35. (New) The data receiving device of claim 32, wherein the executable program is configured to deny to the recipient access to the identified data if authorization to access the identified data is not verified.

36. (New) A computer readable medium, comprising:

an executable program configured to be transmitted along with identified data from a data transmitting device to a data receiving device and to be executed by a processor on the data receiving device when a recipient attempts to access the identified data, the executable program having instructions which cause the processor to verify that one or both of the recipient and the data receiving device are authorized to access the identified data.